



**U.S. Department of Justice**

*United States Attorney  
Southern District of New York*

*The Silvio J. Mollo Building  
One Saint Andrew's Plaza  
New York, New York 10007*

September 18, 2019

**BY ECF (Redacted) and FAX: (212) 805-6737 (Unredacted)**

The Honorable George B. Daniels  
United States District Judge  
Southern District of New York  
500 Pearl Street  
New York, NY 10007

**Re: *United States v. Evaldas Rimasauskas*, 16 Cr. 841 (GBD)**

Dear Judge Daniels:

The Government respectfully submits this letter in advance of the defendant's sentencing, which is scheduled for September 25, 2019 at 10:00 AM, and in response to arguments raised by the defendant in his sentencing submission ("Def. Sentencing Mem."). As discussed in further detail below, over the course of several years, Rimasauskas played a significant role in the perpetration of a major theft of over \$120 million from two U.S.-based multinational technology companies (identified as Victim-1 and Victim-2 in the Indictment) through the use of a business email compromise ("BEC") scheme. For the reasons set forth below, a Guidelines sentence of 97 to 121 months' imprisonment, is sufficient, but not greater than necessary, to achieve the goals of sentencing with respect to the defendant, who was a central player in a long-term and lucrative fraud. The Government further submits that the defendant's requested sentence of time served would fail entirely to serve the essential sentencing goals of providing just punishment, affording general and specific deterrence, and promoting respect for the law.

**Overview of Offense Conduct**

From at least in or 2013 through in or about 2015, Rimasauskas participated in a fraudulent business email compromise scheme which successfully targeted various companies, including Victim-1, Victim-2, and their subsidiary companies (collectively, the "Victim Companies"). Rimasauskas's role in the scheme included, among other things, serving as the sole shareholder and director of a fraudulent company; opening and controlling bank accounts that were used to receive the stolen funds and then send those funds to other bank accounts so as to launder the proceeds of the fraud; and submitting false and fraudulent documents to support the fraud. *See* Final Presentence Investigation Report (June 11, 2019) (Dkt. No. 37) ("PSR") ¶ 15.

**A. Theft from Victim-1**

In furtherance of the scheme, in 2013, Rimasauskas traveled from his home in Vilnius, Lithuania to Riga, Latvia, in order to register himself as a director and sole shareholder of a company (referred to as “Company-2” in the Indictment). The name of the fictitious company in Latvia for which Rimasauskas served as director and sole shareholder was deliberately chosen to be the same exact name as that of a well-known Taiwanese hardware manufacturer (referred to as “Company-1” in the Indictment) that regularly conducts business with many Internet and computer companies, including Victim-1 and Victim-2. Rimasauskas identified himself as both the purported director of the Latvian Company-2, as well as the sole signatory on a bank account at a bank based in Latvia (“Latvian Bank”) in Company-2’s name. *See id.* ¶ 16. The Government’s investigation has established that Company-2 had no legitimate business purpose or operations, and existed only on paper in order to facilitate the scheme in which Rimasauskas engaged: to trick the Victim Companies into believing that bank accounts opened in the name of the fraudulent Latvian Company-2 in fact belonged to the legitimate Taiwanese Company-1, so as to induce the Victim Companies to wire money due to Company-1 to bank accounts controlled by Rimasauskas.

In October 2013, shortly after the bank account for the fraudulent Latvian Company-2 was opened, individuals who worked for Victim-1 received a series of fraudulent phishing emails from purported employees of the true Taiwanese Company-1, stating that the banking information for Company-1 had changed, and asking that Victim-1 direct all future payments to the fraudulent bank account at the Latvian Bank in the name of the fraudulent Latvian Company-2, and which Rimasauskas controlled. As a result of this scheme, between approximately October 10 and October 24, 2013, Victim-1 sent three wire transfers from its bank account at a U.S.-based bank (“U.S. Bank”) to the Latvian Bank Company-2 account, totaling approximately \$23,260,450.17 USD. From there, approximately \$843,855.92 USD was further transferred into another bank account, in the name of a purported South African company at a Latvian bank; further transfers were subsequently made from that Latvian account to other accounts in Latvia, opened in the names of other companies. To facilitate these money laundering activities, Rimasauskas submitted requests to the Latvian Bank to increase the limits on payments that could be made from the fraudulent Quanta Computer account to the other bank accounts. *See id.* ¶ 16.

Upon inquiries as to the status of the payments by the real Taiwanese Company-1 in Taiwan, Victim-1 shortly thereafter realized it had been defrauded, and instructed the U.S. Bank to attempt to cancel the transfers. As a result, the Latvian Bank subsequently froze the funds that remained in the Company-2 bank account due to possible fraud. Rimasauskas, however, submitted a variety of false and fraudulent documents to the Latvian Bank in an effort to unfreeze the funds, and otherwise to establish the purported legitimacy of the fraudulent transfers from Victim-1 to the fraudulent Company-2 account at the Latvian Bank. These false and fraudulent documents included Rimasauskas’s submission of a “Sale Purchase Contract,” which was signed by Rimasauskas on behalf of Company-2, and purportedly by a director of Victim-1 on Victim-1’s behalf. The contract, however, was fraudulent, and the purported signature of the Victim-1 director was forged. Rimasauskas also submitted a letter to the Latvian Bank allegedly

from Victim-1's U.S. bank, stating that the funds were legitimately transferred from Victim-1 to the Company-2 account at the Latvian Bank pursuant to the fraudulent contract, and requesting that the frozen funds be released. That letter, too, was a forgery, on false letterhead. *See id.* ¶ 17.

These activities led to the opening of a formal Latvian law enforcement investigation to determine, whether under Latvian law, Victim-1 had been a victim of fraud and thus entitled to the return of the frozen funds. As part of the investigation, Rimasauskas was questioned by Latvian authorities, and he continued to falsely assert that the Latvian Company-2 was a real company that conducted actual business transactions with Victim-1. The Latvian investigation was transferred to judicial proceedings, and on or about March 19, 2015, Rimasauskas submitted the fraudulent documents to the Latvian courts, in an attempt to establish that the funds at issue were legitimate payments for actual business transactions between Victim-1 and the Latvian Company-2. Nevertheless, on or about April 16, 2015, a Judge of the Riga District Court in Latvia concluded that Victim-1 had been a victim of a fraud, and ordered that the funds that Victim-1 had been tricked into sending to the Latvian Bank account opened by Rimasauskas be returned to Victim-1. *See id.* ¶ 18.

#### **B. Theft from Victim-2**

Despite the Latvian court proceedings and the failure of Rimasauskas and his confederates to regain control over the funds they had stolen from Victim-1, Rimasauskas was not deterred. Rather, he brazenly continued his participation in the scheme, this time targeting Victim-2. Specifically, in June 2015, Rimasauskas traveled to Cyprus in order to open another bank account at a bank based in Cyprus ("Cyprus Bank"), also in the name of the fraudulent Latvian Company-2. To support the opening of the Cyprus Bank account, and to make it appear that Company-2 was a legitimate business, Rimasauskas provided copies of bank statements from the fraudulent Latvian Bank account as well as other fraudulent contracts and invoices purportedly between the Latvian Company-2 and Victim-2 and its subsidiaries. Rimasauskas again served as the signatory and account holder, as a director of the fraudulent Latvian Company-2. *See id.* ¶ 19.

Then, starting in August 2015, fraudulent phishing emails were sent to individuals who worked for Victim-2's accounts payable group, in a manner similar to that which was previously used with Victim-1. These fraudulent emails requested that Victim-2 direct future payments for the Taiwanese Company-1 to the fraudulent Company-2 account at the Cyprus Bank that had been opened by Rimasauskas. Shortly thereafter, between approximately August 21, 2015 and September 14, 2015, Victim-2 and its subsidiaries initiated 16 wire transfers from their U.S.-based bank accounts, totaling \$98,879,545.80 USD. After these funds were wired to the Cyprus Bank account, the funds were further distributed to a variety of bank accounts at banks in Cyprus, Hungary, Latvia, Estonia, Lithuania, Hong Kong, and Slovakia, in the name of various other companies. Although the transfer of the majority of the funds that Victim-2 was tricked into sending to the fraudulent Cyprus Bank account were reversed, approximately \$26,479,079.24 USD were already transferred by the time the fraud had been detected. *See id.* ¶ 20.

### **Procedural History**

On December 22, 2016, a federal grand jury sitting in the Southern District of New York returned and filed an Indictment against Rimasauskas, charging him with the following offenses: in Count One with wire fraud, in violation of Title 18, United States Code, Sections 1349, 1434, and 2; in Count Two with aggravated identity theft, in violation of Title 18, United States Code, Sections 1028A and 2; in Count Three with money laundering, in violation of Title 18, United States Code, Sections 1956(a)(1)(B)(i) and 2; in Count Four with money laundering, in violation of Title 18, United States Code, Sections 1956(a)(2)(B)(i) and 2; and in Count Five with money laundering, in violation of Title 18, United States Code, Sections 1957(a) and 2.

On or about March 15, 2017, Rimasauskas was arrested by Lithuanian authorities as he attempted to enter the country, and has been in custody of law enforcement since. On or about August 16, 2017, Rimasauskas was subsequently extradited to the United States to face charges in this Court, and was detained without prejudice at that time. [REDACTED]

### **Plea Agreement**

On March 29, 2019, Rimasauskas pleaded guilty pursuant to a Plea Agreement to Count One of the Indictment, with a stipulated Guidelines range of 97 to 121 months' imprisonment, based on the intended loss of the scheme, \$122,139,995.97. Further, Rimasauskas agreed to forfeit a sum of \$49,738,559.41, reflecting the sum of money that was in Rimasauskas's control over the course of the fraud, and to pay in restitution a sum of \$26,479,079.24, reflecting the actual loss suffered by the Victim Companies in this case.

### **Applicable Law**

Although *United States v. Booker* held that the Guidelines are no longer mandatory, it also held that they remain in place and that district courts must "consult" the Guidelines and "take them into account" when sentencing. 543 U.S. 220, 264 (2005). As the Supreme Court stated, "a district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range," which "should be the starting point and the initial benchmark." *Gall v. United States*, 552 U.S. 38, 49 (2007).

After that calculation, a sentencing judge must consider seven factors outlined in Title 18, United States Code, Section 3553(a): (1) "the nature and circumstances of the offense and the history and characteristics of the defendant;" (2) the four legitimate purposes of sentencing, as set forth below; (3) "the kinds of sentences available;" (4) the Guidelines range itself; (5) any relevant policy statement by the Sentencing Commission; (6) "the need to avoid unwarranted sentence disparities among defendants;" and (7) "the need to provide restitution to any victims." 18 U.S.C. § 3553(a)(1)-(7); *see also Gall*, 552 U.S. at 50 & n.6.

In determining the appropriate sentence, the statute directs judges to “impose a sentence sufficient, but not greater than necessary, to comply with the purposes” of sentencing, which are:

- (A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;
- (B) to afford adequate deterrence to criminal conduct;
- (C) to protect the public from further crimes of the defendant; and
- (D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner.

18 U.S.C. § 3553(a)(2).

### **A Guidelines Sentence Is Appropriate**

The Government respectfully submits that the application of the statutory sentencing factors set forth in Title 18, United States Code, Section 3553(a) supports the imposition of a Guidelines sentence in Rimasauskas’s case. Given the central role that Rimasauskas played in the opening of the bank accounts into which the fraudulently procured funds from the Victim Companies were wired, his efforts to further launder those funds into other accounts and to recuperate those stolen funds when the Latvian Bank and authorities froze the funds he had stolen, and his decision—after the scheme had been detected as fraudulent against Victim-1—to continue the scheme against Victim-2 using the same means and methods, a below-Guidelines sentence, particularly Rimasauskas’s requested sentence of time served, would not be an appropriate result.

First, a substantial Guidelines sentence is necessary to reflect the nature, circumstances, and seriousness of the offense, to promote respect for the law, and to provide just punishment. *See* 18 U.S.C. § 3553(a)(1), (2)(A). For over two years, Rimasauskas played the key role of a prolific money launderer in a business email compromise scheme that managed to trick two sophisticated multinational technology companies to wire over \$120 million to accounts he controlled. In order to be successful, Rimasauskas had to travel internationally to register the fraudulent Company-2 in Latvia, and to open bank accounts in Latvia and Cyprus, and to facilitate the laundering of funds into and out of those accounts, including by submitting fake and fraudulent documents in an effort to facilitate the transfer of funds into and out of those accounts. And once the fraud was detected, Rimasauskas misled banks and foreign authorities in an effort to regain control over the stolen funds. Although the majority of the stolen funds were returned to Victim-1 and Victim-2, Rimasauskas’s efforts nevertheless resulted in the successful and significant actual loss of over \$26 million dollars to Victim-2.

Second, a substantial sentence is necessary in light of the history and characteristics of this defendant, and to afford adequate deterrence. *See* 18 U.S.C. § 3553(a)(1), (2)(B). As described above, Rimasauskas played a significant role in a substantial and pervasive fraud which resulted in the theft of over \$120 million, of which over \$26 million has not been recovered. Far from an isolated mistake, Rimasauskas’s participation in the scheme spanned years, and the actions he took to ensure its success were involved and varied. Not only did he

agree to serve as a director and sole shareholder of the fraudulent Latvian Company-2—a company for which he undertook no actual business activity aside from ensuring that its bank accounts were open to receive stolen funds—but he then further transmitted those funds to other bank accounts as part of a money laundering scheme. In furtherance of the scheme, he traveled internationally, submitted fraudulent documents with his signature upon them in furtherance of these transfers, made false statements to Latvian police and participated in Latvian court proceedings in an effort to reverse the freezing of funds once his fraud was detected. And when his efforts to reverse the hold placed on the transfer of funds failed with regard to Victim-1, he decided to try all over again with Victim-2, again traveling internationally, representing that the fraudulent Company-2 was a true ongoing business concern which conducted business with international technology companies to the Cyprus Bank, and submitting documents (including bank statements and documents from the Latvian Bank account) in order to open the Cyprus Bank account, all in an effort to continue the success of the scheme. Most tellingly, Rimasauskas did not exit the scheme once the fraud had been uncovered in Latvia. Under such circumstances, specific deterrence as to Rimasauskas is particularly warranted.

General deterrence is an important sentencing interest specifically in the context of the type of fraud charged in the case, to send a message to others who are similarly situated against their continuation of business email compromise scams such as this one. BEC schemes have become a pervasive type of financial crime for transnational criminal organizations operating all over the world, targeting victims in the United States and elsewhere, in part because they are easy to implement and conceal, and profitable when successful. BEC scheme participants can send emails targeting thousands of potential victims each day at nearly no cost while requesting millions of dollars in funds. As a result, victims continue to receive BEC scam emails worldwide on a regular and consistent basis, and the cost to victims of such crimes is significant and growing. *See* FBI News, “Business E-Mail Compromise: Cyber-Enabled Financial fraud on the Rise Globally (Feb. 27, 2017), accessible at <https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise> (“Since January 2015, there has been a 1,300 percent increase in identified exposed losses, now totaling over \$3 billion.”); FBI News, “Worldwide Sweep Targets Business Email Compromise,” Sept. 10, 2019 (“Since the [FBI’s] Internet Crime Complaint Center (IC3) began formally tracking BEC (and its variant, email account compromise, or EAC) in 2013, it has gathered reports of more than \$10 billion in losses from U.S. victims alone. The worldwide tally is more than \$26 billion.”). A sentence within the Guidelines range is especially necessary here to remind BEC scheme participants around the world—both those directly engaging the victims and those who, like the defendant, play a critical role in the scheme by receiving and laundering the crime proceeds—that significant consequences await if and when they are caught.

In this case, Rimasauskas was able to quickly and easily open bank accounts, and with the transmission of emails targeting particular departments at the Victim Companies, Rimasauskas was able to easily receive millions of dollars in a short period of time, and further disburse funds quickly before the fraud could be detected. Following the initial investment in registering the company and falsifying some documents, this crime carried essentially no further costs, apart from the prospect of being arrested and facing criminal penalties. This kind of BEC fraud, perpetrated through social engineering, phishing emails and online banking from a



continent away, through the use of the Internet and the anonymity it provides, is difficult to investigate. Efforts by law enforcement to detect and apprehend individuals engaged in this kind of fraud often taken a substantial time after the crime has occurred, when perpetrators have fled, concealed their participation, or relocated their fraudulent proceeds, and succeed only with the cooperation of international law enforcement and banking authorities. Consequently, general deterrence is needed to counterbalance the fact that social engineering and money laundering schemes such as this one carry low costs and are difficult to solve in a timely fashion, and to remind participants in these types of BEC schemes around the world that significant consequences await if and when they are caught.

Rimasauskas's arguments in support of a time-served sentence are without merit. Although it is true that the Court's assessment of the Section 3553(a) factors may account for both [REDACTED] and the defendant's criminal history (*see* Def. Sentencing Mem. at 7-10), neither should be afforded significant weight in these circumstances, when placed in the context of Rimasauskas's crime. To the extent that Rimasauskas suggests these facts suggest he has been rehabilitated by his arrest and that there is no need for further individual deterrence, it is significant that the defendant's participation in this crime, and his efforts to hide the fraudulent nature of these transactions to banks and authorities lasted over an extended period of time. Perhaps most telling is the fact that, despite Rimasauskas's failed attempts to convince the Latvian Bank, Latvian law enforcement, and courts that the funds stolen were Victim-1 were legitimately earned by his fraudulent Company-2, Rimasauskas was not deterred. Rather, he continued to participate in the scheme, again traveling internationally to Cyprus to open a new fraudulent bank account, and relying on bank statements from the Latvian Bank in an effort to establish the legitimacy of Company-2's business dealings and to support the ruse that Company-2 would be earning large sums of money from business it was conducting with major Internet companies. Rimasauskas also made false statements to Latvian law enforcement over the course of their investigation, as well as false statements to Lithuanian and U.S. law enforcement upon his arrest. [REDACTED]

Under such circumstances, neither [REDACTED] nor the fact that he had no prior criminal convictions justify a below-Guidelines sentence, particularly a sentence of time served.<sup>1</sup>

Rimasauskas also argues that his role in the conspiracy warrants a lesser than Guidelines sentence so as to distinguish him from those with greater roles. (*See* Def. Sentencing Mem. at 6-7). But the cases he cites in support are not cases that support the imposition of a lenient non-Guidelines sentence, but rather are cases in which courts decided to apply a two-point minor role adjustment under U.S.S.G. § 3B1.2(b)—an adjustment that the agreed-to stipulated Guidelines range in the Plea Agreement makes plain that, as a factual matter, does not apply here. Indeed, there is no viable argument that Rimasauskas's role in committing the fraud at issue made him

---

<sup>1</sup> The Government has no objection to the Court taking under advisement Rimasauskas's time while incarcerated in Lithuania awaiting extradition to the United States. (*See* Def. Sentencing Mem. at 10-11).

“substantially less culpable than the average participant” in the scheme, *see* U.S.S.G § 3B1.2(b), app. n.3, so as to warrant such a reduction.

To whatever extent that Rimasauskas relies upon these cases by analogy to assert he is deserving of a sentence below the agreed-upon Guidelines range, Rimasauskas’s case can be easily distinguished from the simple drug couriers that are described in the cases cited by him in support of his argument. For instance, the court in *United States v. Ruiz*, 246 F.2d 263, 271 (S.D.N.Y. 2002) found important that there was “no evidence that Ruiz was a longstanding member of the conspiracy with a regular role” but rather “was recruited specifically for the purpose of accepting delivery of [a] particular shipment of drugs,” and whose “responsibility after taking delivery was at most simply to count the pills and then turn them over.” *Id.* at 271-72 (applying minor participant role adjustment, but describing it as a “close case,” and nevertheless sentencing Ruiz to 97 months’ imprisonment, which was the top of the 78 to 97 month Guidelines range) (cited at Def. Sentencing Mem. at 6). By contrast, there is ample evidence of Rimasauskas’s ongoing and longstanding participation in the conspiracy at hand over the course of at least two years, and his decision to continue his participation even after the detection of the fraud against Victim-1 by the banks, Latvian law enforcement, and Latvian courts. By virtue of his decision to act as the purported director of the fraudulent Latvian Company-2—a company which he understood had no business purpose—and to open bank accounts in its name and help in efforts to facilitate the transfer of funds from two different victims into and out of the bank accounts he controlled, Rimasauskas was not “essentially fungible” to the enterprise, *contra United States v. Fernandez*, 312 F. Supp. 2d 522, 524 (S.D.N.Y. 2004) (concluding two-level minor role decrease applied to defendant who couriered drugs but lacked knowledge about the drug type and quantity involved, had no decision making authority, and had no relationship or commitment to other co-conspirators) (cited at Def. Sentencing Mem. at 6). Nor is Rimasauskas’s significant role in the scheme comparable to that of the safety-valve eligible defendant in *United States v. Sanchez*, 925 F. Supp. 1004 (S.D.N.Y. 1996), who acted like a “novice in handling” a sole drug transaction on behalf of principles and co-conspirators he did not know, *id.* at 1008-09. Because Rimasauskas had an ongoing “relationship [with] other participants in the scheme”; his actions were “importan[t] to the success of the venture,” as he was the only individual who represented himself as the owner and director of the fraudulent Company-2 and asserted that it was an ongoing business concern; and he was aware of the full “nature and scope of the criminal enterprise,” he was not a minor participant in this scheme. *United States v. Garcia*, 920 F.2d 153, 155 (2d Cir. 1990) (*per curiam*).



**Conclusion**

The defendant engaged in serious criminal conduct, involving a direct, significant, and leading role in the theft of over \$120 million from U.S. companies. Under such circumstances, a significant incarceratory sentence within the Guidelines range is appropriate, but not greater than necessary, to serve the ends of sentencing—including promoting respect for the law, providing just punishment for this particular defendant, and serving the needs of both specific and general deterrence.

Respectfully submitted,

GEOFFREY S. BERMAN  
United States Attorney

By:

A handwritten signature in black ink, reading "Eun Young Choi", written over a horizontal line.

Eun Young Choi  
Olga Zverovich  
Assistant United States Attorneys  
Southern District of New York  
(212) 637-2187/2514

cc: Defense Counsel (via email)